Atty. Docket No.: 3460-Z *AF* *SFN*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

re application of

Leon Benhamou

Serial No. 10/695,952   Group Art Unit 2155

Filed: October 30, 2003   Examiner Vitali A. Korobov

For: Method and Apparatus for Securing Network
Management Communications

APPEAL BRIEF TRANSMITTAL

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Attached hereto is the BRIEF ON APPEAL for the above-identified application. Please charge the fee in the amount of $500 to the undersigned attorney's deposit account No. 26-0090.

It is requested that a two-month extension of time be granted under the provisions of 37 C.F.R. §1.136(a) to extend the period for filing this Brief on Appeal. Please charge the fee in the amount of $450 to the undersigned attorney's deposit account No. 26-0090.

Any additional fees necessary to effect the proper and timely filing of this Brief may be charged to Deposit Account No. 26-0090.

Respectfully submitted,

Jim Zegeer

Jim Zegeer, Reg. No. 18,957
Attorney for Appellant

Attachment: Brief on Appeal

Suite 108
801 North Pitt Street
Alexandria, VA 22314
Telephone: 703-684-8333

Date: October 2, 2006

In the event this paper is deemed not timely filed, the applicant hereby petitions for an appropriate extension of time. The fee for this extension may be charged to Deposit Account No. 26-0090 along with any other additional fees which may be required with respect to this paper.

Atty. Ref. 3460-Z

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of

Leon Benhamou

Serial No. 10/695,952   Group Art Unit 2155

Filed: October 30, 2003   Examiner Vitali A. Korobov

For: Method and Apparatus for Securing Network
Management Communications

BRIEF ON APPEAL

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the final rejection mailed December 2, 2005 finally rejecting claims 1 - 18 of the above-identified application.

(i). The Real Party in Interest

The real party in interest is Alcatel.

(ii). Related Appeals and Interferences

There are no related appeals or interferences.

(iii). Status of the Claims

Claims 1 - 18, the only claims pending in the application, stand finally rejected.

(iv). Status of the Amendments

There were no amendments filed subsequent to the final rejection.

(v). Summary of Claimed Subject Matter

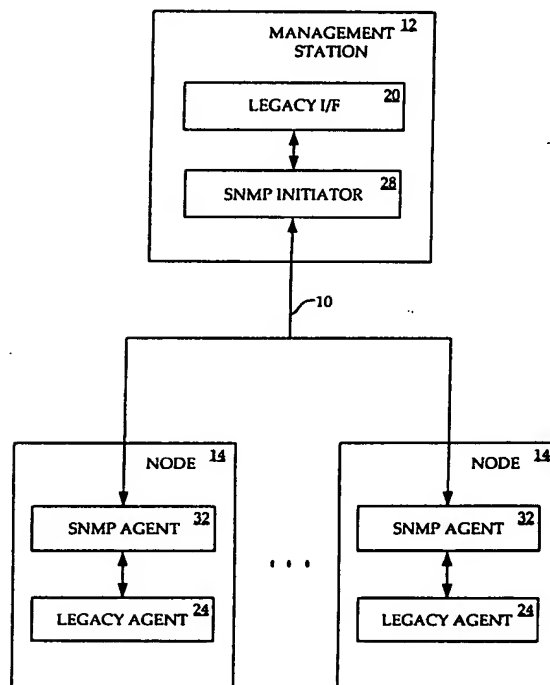Figure 1 of the drawings is reproduced for convenience of reference as follows:

FIG. 1

The network 10 includes a management station 12 and a plurality of nodes 14, the management station 12 being responsible for administering the nodes 14. The management station 12 exchanges network management messages with each node 14 by transmitting and receiving network management messages over the network 10. Collectively, the management station 12 and the nodes 14 are referred to as network elements. The management station 12 includes a legacy management interface 20, and each node includes a legacy agent 24. The legacy management interface generates legacy network management messages, to which each legacy agent 24 has the ability to respond. Each legacy agent 24 may respond to particular legacy network management messages by generating another legacy network management message, which the legacy management interface has the ability to process. Each legacy agent 24 may also generate unsolicited legacy network management messages in order to, for example, report state changes or status changes. (Specification, page 5, first full paragraph.)

The management station 12 and the nodes 14 exchange legacy network management messages using a secure version of Simple Network Management Protcol (SNMP), such as SNMPv3. The legacy network management messages are embedded within SNMP messages as user-defined SNMP objects. The management station 12 includes an SNMP initiator 28. The SNMP initiator 28 receives a legacy network management message generated by the legacy interface 20, and embeds the legacy network management message within an SNMP message. The

SNMP initiator 28 then transmits the SNMP message to one or more of the nodes 14. (Specification, page 5, second full paragraph.)

Each node 14 includes an SNMP agent 32 which receives an SNMP message from the SNMP initiator 28. The SNMP message includes as a user-defined object a legacy network management message generated by the legacy management interface 20 and embedded within the SNMP message by the SNMP initiator 28. The SNMP agent 32 extracts the legacy network management message from the SNMP message and passes it to the legacy agent 24 within the node 14. The legacy agent 24 processes the legacy network management message in accordance with the legacy management protocol. If the legacy agent 24 prepares a second legacy network management message in response to the legacy network management message generated by the legacy interface 20, the legacy agent 24 passes the second legacy network management message to the SNMP agent 32. The SNMP agent 32 embeds the second legacy network management message as a user-defined object within an SNMP message, and sends the SNMP message to the SNMP initiator 28. Likewise, if the legacy agent 24 generates an unsolicited legacy network management message, the legacy agent 24 passes the legacy network management message to the SNMP agent 32. The SNMP agent 32 embeds the legacy network management message as a user-defined object within an SNMP message, and sends the SNMP message to the SNMP initiator 28. (Specification, paragraph bridging pages 5 and 6.)

The method and apparatus of the present invention allow legacy network management messages to be transmitted with improved security, without requiring replacement of an entire legacy system. Using simple SNMP initiators and simple SNMP agents, legacy network management messages are embedded within SNMP messages and exchanged between network elements using a secure version of SNMP. Legacy software, in the form of agents and interfaces, is then able to process the legacy management messages.

In compliance with 37 C.F.R. 41.37(V), the steps in claims 1 - 6 have been annotated to make specific reference to the specification where they find support. There are no "means" clauses in claims 7 - 18.

1. A method of providing secure network management communications within a communication network, the communication network including a plurality of network elements each adapted to generate and process legacy network management messages in conformance with a legacy management system, the method comprising the steps of:
embedding a first legacy network management message within a first Simple Network Management Protocol (SNMP) message at a first network element; (page 3, second full paragraph; page 5, second full paragraph; abstract.)
transmitting the first SNMP message over the network to a second network element; and (page 3, second full paragraph, abstract.)
extracting the first legacy network management message from the first SNMP message at the second network element. (paragraph bridging pages 5 and 6; page 6, first full paragraph.)

2. The method of claim 1 wherein the step of transmitting the first SNMP message comprises transmitting the first SNMP message in conformance with a secure version of SNMP. (page 6, last full paragraph.)

3. The method of claim 2 wherein the step of transmitting the first SNMP message comprises transmitting the first SNMP message in conformance with

SNMP version 3 (SNMPv3). (page 5, second full paragraph; abstract.)

4.   The method of claim 1 wherein the legacy management system provides less security than SNMP. (page 7, second full paragraph, second sentence.)

5.   The method of claim 1 comprising the further steps of:
    generating the first legacy network management message at the first network element; and (page 5, first full paragraph, last two sentences.)
    processing the first legacy network management message at the second network element. (page 6, second sentence from top of page.)

6.   The method of claim 5 comprising the further steps of:
    generating a second legacy network management message at the second network element in response to the first legacy network management message; (page 6, third sentence from top of page.)
    embedding the second legacy network management message within a second SNMP message at the second network element; (page 6, fourth sentence from top of page.)
    transmitting the second SNMP message over the network to the first network element; and (page 6, fourth sentence from top of page.)
    extracting the second legacy network management message from the second SNMP message at the first network element. (page 6, first full paragraph.)

        (vi). Grounds of Rejection to be Reviewed on Appeal

Ground No. 1

The rejection of claims 1, 2, 4-10 and 12-12 under 35 U.S.C. 102(e)

as being anticipated by Andrews (US 6,697,845) (hereinafter

Andrews).

Ground No. 2

The rejection of claims 3 and 11 under 35 U.S.C. 103(a) as being

unpatentable over Andrews.

(vii).   Argument

<u>As to Ground No. 1</u>

It is respectfully requested of the rejection of claims 1, 2,

4-10 and 12-18 under 35 U.S.C. §102(e) as being anticipated by

Andrews 6,697,845) is clearly erroneous.

In his Background of Invention, Andrews states:

> Several shortcomings and deficiencies exist in the con-
> ventional solutions to provide support of multiple SNMP
> agents in a single element. For example, it is required that
> the SNMP manager be aware that it is communicating with
> multiple processing entities, i.e., agents, associated with the
> managed element. Further, the manager may have to switch
> between community strings based on what it needs to
> retrieve. Also, the manager has to be re-configured each time
> when it switches between two community strings or between
> two independent, non-community agents. Thus, the purpose
> of managing the element as a single managed node is
> thwarted because the manager does not "see" the node as
> single platform, rather as a partitioned collection of agents.
> Additionally, conventional community string-based
> multi-agent solutions do not easily adapt to the Agent
> Extensibility (AgentX) standard which allows for multiple
> subagents to be registered with a common master agent that
> is seen as a single SNMP entity by the manager.

These are the shortcomings that Andrews sought to solve.

Furthermore, in his Summary of the Invention, column 2, lines

36-48, Andrews states:

> An SNMP master agent and one or more subagents are
> provided for managing the <u>node, which use the AgentX</u>
> <u>protocol for communication therebetween</u>. At least a
> portion of a Management Information Base (MIB) associated

with the management functionality of the managed node is
supported by an SNMP peer agent that is <u>proxied via an
AgentX subagent (PSA). The PSA registers the MIB
portion with the SNMP master agent via an AgentX
registration message</u>. When an SNMP manager sends an SNMP
management request to the SNMP master agent, the SNMP
master agent <u>parses the SNMP</u> management request <u>into one
or more AgentX protocol messages</u> depending upon the
subagents involved.   [Emphasis added.]

Appellant's claim 1 recites:

...embedding a first legacy network management message
within a first Simple Network Management Protocol (SNMP)
message at a first network element;

    transmitting the first SNMP message over the network
to a second network element; and

    extracting the first legacy network management
message from the first SNMP message at the second network
element.

It can be seen therefore that this is the <u>exact opposite</u> of the

Andrews patent.   Andrews is using an AgentX to transport SNMP

management information, and appellant's invention is concerned with

using SNMP management to transport AgentX.   The "wrapper" reference

referred to by the Examiner (column 4, line 31) does not change

this fundamental difference.   Note the claim language reads:

"embedding a first legacy network management message within a first

Simple Network Management Protocol (SNMP) message...."   Clearly,

Andrews uses AgentX protocol for communication.

    The Examiner seeks to modify the express disclosure of Andrews

by referring to "RFC2741-agent extensibility (AgentX) protocol

version 1" at page 10 of the Final Rejection.

Appellant's claims deal with <u>legacy network management messages embedded in a first simple SNMP message</u>. The RFC2741 protocol does not refer to legacy network management messages.

In appellant's claim 9, the language reads:

> a Simple Network Management Protocol (SNMP) initiator at the management station for embedding the first legacy network management message <u>within</u> a first SNMP message and for transmitting the first SNMP message to the node....

Again, this language distinguishes from Andrews in that it denotes the opposite of the Andrews situation.

In appellant's claim 13, the operative language is:

> instructions <u>for embedding the legacy network management message within an SNMP message</u>...

and this is not taught or suggested by Andrews. In fact, the opposite is taught.

In appellant's claim 15, note the language reading:

> instructions for extracting a first legacy network management message from the first SNMP message, the first legacy network management message conforming to a legacy network management protocol....

Clearly, this is not the case with Andrews.

In view of the above, further and favorable reconsideration is respectfully requested.
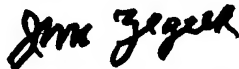

As to Ground No. 2

The rejection of claims 3 and 11 under 35 U.S.C. 103(a) as being unpatentable over Andrews is clearly in error.

Claim 3 depends from claim 1, and claim 11 depends from claim 9 and are patentable for the reason given above.

CONCLUSION

In view of the above, the Examiner clearly erred in rejecting claims 1 - 18 and should be reversed.

Respectfully submitted,

[signature]

Jim Zegeer, Reg. No. 18,957
Attorney for Appellant

Attachment: CLAIMS APPENDIX
                EVIDENCE APPENDIX

Suite 108
801 North Pitt Street
Alexandria, VA 22314
Telephone: 703-684-8333

Date: October 2, 2006

In the event this paper is deemed not timely filed, the applicant hereby petitions for an appropriate extension of time. The fee for this extension may be charged to Deposit Account No. 26-0090 along with any other additional fees which may be required with respect to this paper.

(viii)   CLAIMS APPENDIX

1.   A method of providing secure network management communications within a communication network, the communication network including a plurality of network elements each adapted to generate and process legacy network management messages in conformance with a legacy management system, the method comprising the steps of:

embedding a first legacy network management message within a first Simple Network Management Protocol (SNMP) message at a first network element;

transmitting the first SNMP message over the network to a second network element; and

extracting the first legacy network management message from the first SNMP message at the second network element.

2.   The method of claim 1 wherein the step of transmitting the first SNMP message comprises transmitting the first SNMP message in conformance with a secure version of SNMP.

3.   The method of claim 2 wherein the step of transmitting the first SNMP message comprises transmitting the first SNMP message in conformance with SNMP version 3 (SNMPv3).

4.   The method of claim 1 wherein the legacy management system provides less security than SNMP.

5.   The method of claim 1 comprising the further steps of:

generating the first legacy network management message at the first network element; and

processing the first legacy network management message at the second network element.

6.   The method of claim 5 comprising the further steps of:

generating a second legacy network management message at the second network element in response to the first legacy network management message;

embedding the second legacy network management message within a second SNMP message at the second network element;

transmitting the second SNMP message over the network to the first network element; and

extracting the second legacy network management message from the second SNMP message at the first network element.

7. The method of claim 1 wherein the first network element is a management station, and wherein the second network element is a node.

8. The method of claim 1 wherein the first network element is a node, and wherein the second network element is a management station.

9. A network management system within a communication network, the communication network including a management station and a node, comprising:

a legacy interface at the management station for generating a first legacy network management message in conformance with a legacy network management protocol;

a Simple Network Management Protocol (SNMP) initiator at the management station for embedding the first legacy network management message within a first SNMP message and for transmitting the first SNMP message to the node;

an SNMP agent at the node for receiving the first SNMP message and for extracting the first legacy network management message from the first SNMP message; and

a legacy agent at the node for processing the legacy network management message in conformance with the legacy network management protocol.

10.   The system of claim 9 wherein the SNMP initiator is adapted to transmit the first SNMP message in conformance with a secure version of SNMP.

11.   The system of claim 10 wherein the SNMP initiator is adapted to transmit the first SNMP message in conformance with SNMP version 3 (SNMPv3).

12.   The system of claim 9 wherein the legacy network management protocol provides less security than SNMP.

13.   A Simple Network Management Protocol (SNMP) initiator at a management station within a communication network, comprising:
        instructions for receiving a legacy network management message which conforms to a legacy network management protocol;
        instructions for embedding the legacy network management message within an SNMP message; and
        instructions for transmitting the SNMP message to a node within the communication network.

14.   The SNMP initiator of claim 13 wherein the legacy network management protocol provides less security than SNMP.

15.   A Simple Network Management Protocol (SNMP) agent at a node within a communication network, comprising:
        instructions for receiving a first SNMP message from a management station within a communication network;
        instructions for extracting a first legacy network management message from the first SNMP message, the first legacy network management message conforming to a legacy network management protocol; and
        instructions for sending the first legacy network management message to a legacy agent at the node.

16. The SNMP agent of claim 15 wherein the legacy network management protocol provides less security than SNMP.

17. The SNMP agent of claim 15 further comprising:
    instructions for receiving a second legacy network management message from the legacy agent;
    instructions for embedding the second legacy network management message within a second SNMP message; and
    instructions for transmitting the second SNMP message to the management station.

18. The SNMP agent of claim 17 wherein the legacy network management protocol provides less security than SNMP.

(ix). EVIDENCE APPENDIX

None.

(x).   RELATED PROCEEDINGS APPENDIX

There are no proceedings as mentioned in section (i) above, and accordingly no decisions rendered.